DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8/13/2009 has been entered.

2. This action is responsive to communications: application 10/566,584 filed on 1/31/2006; RCE filed on 8/13/2009.

3. Claims 1, 2, 3, 5, and 16 are amended. Claims 8, 11, and 18 have been canceled.

4. Applicant's arguments with respect to claims 1 and 8 have been considered but are moot in view of the new ground(s) of rejection.

Drawings

5. The informal drawings are not of sufficient quality to permit examination. Accordingly, replacement drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to this Office action. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the

examiner, the applicant will be notified and informed of any required corrective action in the next Office action.

Applicant is given a TWO MONTH time period to submit new drawings in compliance with 37 CFR 1.81. Extensions of time may be obtained under the provisions of 37 CFR 1.136(a). Failure to timely submit replacement drawing sheets will result in ABANDONMENT of the application.

Claim Objections

6. Claim 1 is objected to because of the following informalities:

the "receiving a private identification PrivID from the subscriber, the PrivID being correlated with a pre-recorded ID of the subscriber and stored together a subscriber database" (lines 8-9) should apparently read as "the PrivID being correlated with a pre-recorded ID of the subscriber and stored together in a subscriber database"; also the acronym "SIP" is used without spelling out at its first occurrence in the claim.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject

matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. **Claims 1, 3-5, 7, 9-12, 14, 16, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Skog et al. (US Patent no.: 6977917, hereinafter Skog), in view of Enzmann et al (US Pub. No.: US 2004/0136398 A1, hereinafter Enzmann)**.

As per claim 1, Skog discloses "*a method for transparent access authentication of subscribers connected to an authenticating network domain by a General Packet Radio Service GPRS core network or an Universal Mobile Telecommunication System UMTS network, comprising*" (col. 2, lines 25-29, associating a mobile terminal's temporarily assigned IP with a MSISDN number for use with authentication within a service network. Skog discloses the service network is a GPRS network in col. 5, lines 43-45):

"*receiving a context creation request from a subscriber*" (col. 4, lines 28-31, the mobile terminal transmits a message to the access server in order to establish a connection);

"*assigning an IP address to the context*" (col. 3, lines 63-65, the mapping session database includes a plurality of storage locations for an assigned temporary IP address and an associated MSISDN of the mobile terminal; also in col. 4, lines 54-57, the IP address is dynamically allocated to the mobile terminal by the access server or the RADIUS server during the connection setup); "*receiving a check-in ID from the subscriber*" (col. 4, lines 33-35, the mobile terminal transmits authentication information including the user ID);

"receiving a check-in ID from the subscriber" (col. 4, lines 49-67, wherein MSISDN address corresponding with check-in ID);

"*receiving a private identification PrivID from the subscriber, the PrivID is being correlated with a pre-recorded ID of the subscriber in a subscriber database*" (col. 4, lines 58-64, wherein PrivID corresponding with IP address, and Skog also discloses the pre-recorded ID as the IP address and the MSIDSN are stored as record with in a database in col. 4, lines 62-64); *and*

"comparing the check-in ID with the pre-recorded ID, authenticating the subscriber when the check-in ID matches the pre-recorded ID" (col. 5, lines 9-12, the MSISDN of the mobile terminal is determined by examining the mapping session database; col. 5, lines 13-14, and fig. 3, step 130 and 138, wherein authenticating the subscriber corresponding with permitting mobile terminal 45 to access application 85).

However, Skog does not disclose:

"*providing a routing module (7) as a standard entry point for all messages and deciding, in the routing module (7), by evaluation of the PrivID, which network node will handle the message, wherein when a protocol other than SIP is found, the message is routed to a proxy server*".

Enzmann discloses:

"*providing a routing module (7) as a standard entry point for all messages and deciding, in the routing module (7), by evaluation of the PrivID, which network node will handle the message, wherein when a protocol other than SIP is found, the*

message is routed to a proxy server" (page, 4, para. [0048] [0049] [0050], wherein smart router 504 corresponding with router module, the information that parsed from incoming data to determine the data type are corresponding with PrivID; in the first determination step, depending on the information included in incoming data, it can be determined that the data is in a SIP, IP or an Analog fax format, then pass to different network node, see fig. 5, Smart Router 504, and PSTN world 100. Para. [0032], also in figs. 1, 2, and 5, the information passing to different home network nodes, for example, PSTN world, PSTN devices, or IP devices).

Skog and Enzmann are analogous art because they are from the same field of endeavor of telecommunication network including wireless communication.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the steps of authentication mobile terminal as described by Skog and add providing a smart router to route the incoming data packets to different nodes in the network for further processing as taught by Enzmann because it would provide systems and methods for recognizing the type of incoming PSTN signal (see Enzmann, page 1, [0014]).

As per claim 3, Skog discloses "*the method according to claim 1, further comprising: using a Gateway GPRS Support Node to receive the context creation request*" (fig. 2, reference numbers 50 and 60; and col. 3, lines 35-38, the RADIUS Accounting server sends back an acknowledgment that the Accounting Start packet has been received. Since Skog discloses the access server can be implemented in GGSN (GPRS Gateway Serving Node), then the Accounting Start packet can be

received by using GPRS Gateway Serving Node); "*querying the context request to a Radius server*" (col. 3, lines 63-65, the mapping session database includes a plurality of storage locations for an assigned temporary IP address and an associated MSISDN of the mobile terminal); "*using the Radius server to receive the check-in ID*" (col. 4, lines 1-6, RADIUS accounting messages is to be delivered to RADIUS Accounting server. The information in the packet includes MSISDN number and the IP address of the mobile terminal etc); "*and storing the IP address and the check-in ID in a session database*" (col. 4, lines 4-6, the information within a packet of relating to IP address and MSISDN number is used to update the database).

As per claim 4, Skog discloses "*the method according to claim 1, further comprising: a proxy server to compare the check-in ID with the pre-recorded ID, wherein the subscriber database is an application domain database*" (col. 5, lines 6-12, the WAP gateway determine the IP address of the mobile terminal by examining the IP packet header. The MSISDN of the mobile terminal is determined by examining the mapping session database and the associated IP address).

As per claim 5, "*the method according to claim 1, further comprising: using a Radius server to compare a subscriber's IP address in an IP network layer with the assigned IP address*" (col. 5, lines 6-9, the WAP gateway may determine the IP address of the mobile terminal by examining the IP packet header to determine the IP address of the mobile terminal).

As per claim 7, Skog discloses "*the method according to claim 1, comprising the steps of, in all subsequent messages arriving at the proxy server (5), checking for a match of IP address in the IP packet overhead field for source address with that in the application layer protocol header fields and verifying the matching pairs against the IP address assigned by the Radius server (2)*" (col. 5, lines 1-9, once the connection is established, the WAP gateway may determine the IP address of the mobile terminal by examining the IP packet header to determine the IP address of the mobile terminal).

As per claim 9, Skog discloses "*a system of units in a mobile telecommunication network, comprising: characterized at least a first authentication unit connected to a session database via a first data line*" (Fig. 2, RADIUS Server in MSC/VLR; and col. 4, 31-36, mobile terminal requests a access to access server 60, the access server using a password authentication procedure to authenticate the mobile terminal. Since user transmits its user ID and password to access server, there must be a database related to access server for user ID and password information included in the request to be authenticated)*; a second unit connected to the session database via a second data line; wherein the second unit assembles data according to the method of claim 1*" (Fig. 2, RADIUS accounting server 75 and DB 118; col. 4, lines 58-64, the WAP gateway as an accounting request message to enable mapping between identifiers. The IP address and the MSISDN are stored as a record).

As per claim 10, Skog discloses "*the system of units according to claim 9, wherein the first authentication unit comprises a registration server*" ((Fig. 2, RADIUS Server in MSC/VLR. The RADIUS Server/access server appears to be a registration server).

As per claim 12, Skog discloses "*the system of units according to claim 9, wherein the second unit comprises a proxy server*" (col. 5, lines 6-9, the WAP gateway may determine the IP address of the mobile terminal 45 by examining the IP packet header to determine the IP address of the mobile terminal. It describes the functionality of proxy servers. Also in col. 1, lines 54-59, Skog implies the proxy server has been implemented within WAP network).

As per claim 14, Skog discloses "*the system of units according to claim 13, wherein the second unit is connected to a subscriber database*)" (Fig. 5, the authentication unit is connected to Users DB which includes the information of subscriber).

As per claim 16, Skog discloses "*the method of claim 1, wherein the check-in ID is one of an Mobile Station ISDN Number MSISDN and an International Mobile Subscriber Identity IMSI received from the subscriber*" (col. 4, lines 58-62, the MSISDN of the mobile terminal are transmitted over the PPP connection from the access server to the WAP gateway), "*and the pre-recorded ID is one of the subscriber's MSISDN and IMSI pre-recorded in a subscriber database*" (col. 4, lines 62-64, the IP address and MSISDN are stored as a record within the mapping session database).

As per claim 17, Skog discloses "*the system according to claim 12, wherein the proxy server (5) is connected to a subscriber database (4)* " (col. 5, lines 6-12, the WAP gateway determine the IP address of the mobile terminal by examining the IP packet header. The MSISDN of the mobile terminal is determined by examining the mapping session database and the associated IP address).

7. **Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Skog, in view of Enzmann, and further in view of Chaudhary et al. (US 7155526, hereinafter Chaudhary)**.

As per claim 2, Skog in view of Enzmann discloses *claim 1;* however, Skog in view of Enzmann does not specifically disclose the "*wherein the step of authenticating the subscriber includes an A3/A8 algorithm based on an end devices SIM card*".

Chaudhary discloses it as verifying user equipment by sending RAND to SIM card and get a response generated by the GSM algorithm A8 and then establish PDP context message to GGSN over GTP control protocol (col. 11, lines 36-48, col. 12, lines 11-19, and Figure 5).

Skog, Enzmann and Chaudhary are analogous art because they are from the same field of endeavor of wireless network communication.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the authentication mobile terminal with routing different type of incoming data to corresponding notes as described by Skog in view of Enzmann,

and add indicating the packets are in PDP context data and the authentication method is A8 algorithm as described by Chaudhary, because it would provide for the purpose of deploying a standard authentication algorithm such as A8, since standard algorithms are broadly developed, tested and deployed and consequently makes the system developments easier and more efficient (see Chaudhary, col. 11, lines 36-48, col. 12, lines 11-19, and Figure 5).

8. **Claims 6, 13, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Skog, in view of Enzmann, and further in view of Pirttimaa et al (US 0154400 A1, hereinafter Pirttimaa).**

As per claim 6, Skog discloses "*wherein the IP address given in the headers was already checked for a match with the assigned IP address*" (col. 4, lines 51-54, after the connection is established between the access server and the mobile terminal, the only information included in the IP packets that been transmitted is the IP address. Since the IP is the IP address has been assigned to, there is a match for the IP).

However, Skog in view of Enzmann does not explicitly disclose "*using a proxy server to parse an application layer for IP addresses given in headers of registration messages and to compare with the assigned IP address for a match*".

Pirttimaa discloses it as comparing the source address, since the source address indicated in the SIP message corresponds to a "true" source address, e.g. the actual source address of the IP datagram indicated by the stored at the P-CSCF

(page 3, [0043]). Since the source address has been extracted from the SIP message, the parsing process must be taken in place. The SIP message indicates the parsing is in an application layer.

Skog, Enzmann, and Pirttimaa are analogous art because they are from the same field of endeavor of wireless network communication.

It would have been obvious to one of ordinary skill in the art at the time to modify the authentication process of matching application layer IP address as discussed in Skog in view of Enzmann, and add the detail description of a proxy server parses IP address from application layer as described by Pirttimaa because it would provide the purpose of offering the complete details about how the process has been accomplished (see Pirttimaa, page 3, [0042]).

As per claim 13, Skog in view of Enzmann discloses claim 9, but Skog does not disclose "*the system of units according to claim 9, wherein the second unit comprises a proxy server connected to a Proxy Call State Control Function via a routing module*".

Pirttimaa discloses "*the system of units according to claim 9, wherein the second unit comprises a proxy server connected to a Proxy Call State Control Function via a routing module*" (Fig. 3, modules 31 and 33; Fig. 4, modules 31 and 33; page 3, [0043], lines 1-9, based on the result of the address comparison, the P-CSCF makes a forwarding decision. If the compared IP address indicates the same location no fraudulent attack can be assumed. The IP comparison and forward the

data packets to P-CSCF unit implies the existence of proxy server and the routing module).

Skog, Enzmann, and Pirttimaa are analogous art because they are from the same field of endeavor of wireless network communication.

It would have been obvious to one of ordinary skill in the art at the time to modify the authentication process of matching application layer IP address as discussed in Skog in view of Enzmann, and add the detail description of a proxy server parses IP address from application layer as described by Pirttimaa because it would provide the purpose of offering the complete details about how the process has been accomplished (see Pirttimaa, page 3, [0042]).

As per claim 15, Pirttimaa discloses "*the system of units according to claim 13, wherein a routing module selects messages from one of the proxy server and the Proxy Call State Control Function by evaluating the PrivID*" (page 3, lines 1-4, based on the result of the address comparison. The address appears to be a user/attacker's private ID).

Response to Arguments

10. Applicant's arguments with respect to claims 1 and 8 from page 7-8 of last filling have been considered but are moot in view of the new ground(s) of rejection.

Examiner Notes

11. Examiner has pointed out particular references contained in the prior arts of record and in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable to the limitations of the claims. It is respectfully requested from the applicant, in preparing for response, to consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the Examiner.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JING SIMS whose telephone number is (571)270-7315. The examiner can normally be reached on 7:30am-5:00pm EST, Mon-Thu.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JING SIMS/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437